AO-106 (Rev. 06/09)-Application for Search Warrant

FILED

DEC 11 2024

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of a Google Pixel 6a taken off of the person of Robin Black incident to his arrest, IMEI No. 351990802920121, Currently Stored at a Secured Facility Controlled by the Tulsa Police Department

Case No. 24-mj-761-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
7 U.S.C. § 2024(b)	**Benefits Fraud**

The application is based on these facts: ***See*** **Affidavit of USDA Special Agent Erika Skaggs**

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

ERIKA SKAGGS

Digitally signed by ERIKA SKAGGS
Date: 2024.12.10 10:56:25 -06'00'

Applicant's signature

USDA-OIG Special Agent Erika Skaggs

Printed name and title

Subscribed and sworn to by phone.

Date: 12/11/24

Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of a Google Pixel 6a taken off of the person of Robin Black incident to his arrest, IMEI No. 351990802920121, Currently Stored at a Secured Facility Controlled by the Tulsa Police Department	**Case No.**

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Special Agent Erika Skaggs, being first duly sworn under oath, depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C). Therefore, I am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of federal officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the United States Department of Agriculture –

Office of Inspector General (USDA-OIG). I have been so employed since June 2023. I am currently assigned to the Oklahoma Resident Office in the Southwest Region. Prior to holding this position, I was a Special Agent of the Internal Revenue Service—Criminal Investigation (IRS-CI). I was so employed from January 2002 through June 2023. As a Special Agent, some of my functions include investigating individuals engaged in activities constituting criminal violations against the USDA and other related offenses. My duties include conducting criminal investigations into fraud, waste, and abuse within the programs and operations of the USDA. I earned a Bachelor of Science degree in Finance at Oral Roberts University, while working for Bank of America and Arvest State Bank in Tulsa, Oklahoma. I also graduated from the Special Agent Basic Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and knowledge of the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 7 U.S.C. § 2024(b) – Benefits Fraud, will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

5. Under 7 U.S.C. § 2024(b), the government is required to prove the following elements beyond a reasonable doubt:

First: the defendant used, transferred, acquired, altered, or possessed food stamp coupons or authorization cards in a way that was contrary to the law or Department of Agriculture regulations;

Second: the defendant knew he acted contrary to the law or Department regulations; and

Third: the food stamp coupons or authorization cards had a value of $100.00 [or $5,000.00] or more.

See Tenth Circuit Pattern Instruction 2.01 (2021)

Identification of the Device to be Examined

6. The property to be searched is a Google Pixel 6a taken off of the person of Robin Black incident to his arrest, hereinafter the "Device." The Device is currently located at a secured facility controlled by the Tulsa Police Department.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

8. On May 6, 2024, officers with the Tulsa Police Department ("TPD") and the Oklahoma Department of Human Services ("DHS") conducted an undercover operation in response to information received regarding potential food stamp fraud (part of operation "Stamp Out").

9. Over the previous 6-8 months, officers received tips about a black male, later identified as Robin Christopher Black ("Black"), selling government-funded cell phones, but also buying Special Nutrition Assistance Program ("SNAP") Electronic Benefit Transfer ("EBT") cards from indigent and homeless citizens. Among other things, the tips indicated that the individual drove a black Cadillac sedan and that the conduct was occurring at a downtown Tulsa Transit bus stop at 319 South Denver Avenue, Tulsa, Oklahoma, 74103, which is within the Northern District of Oklahoma.

10. Officers surveilled the location in advance of the undercover operation and observed heavy foot traffic to and from the suspected vehicle. Officers also saw multiple hand-to-hand transactions between the suspect and individuals at the bus stop. The undercover operation was conducted based on the tips and the direct observation by law enforcement.

11. At the outset of the operation, TPD Lt. Ian Adair drove an undercover agent, DHS Special Agent Idalia Harris, to the area and dropped her off about two blocks away from the bus stop, on Third Street between South Cheyenne Ave. and

South Boulder Ave. Lt. Adair and other officers then surveilled the bus stop, where they saw Black arrive in the suspected vehicle.

12. Officers watched the undercover agent as she engaged a group of people outside of the bus station. Minutes later, officers observed Black approach the undercover agent. Black and the undercover agent interacted with one another for several minutes. During this time, officers watched the undercover agent and Black walk back to Black's car, where he accessed the front passenger area and the trunk.

13. The undercover agent later clarified that she specifically asked a female at the bus station if she knew anybody who would help her out by buying her SNAP benefits. The female made a phone call, and Black arrived minutes later. The undercover agent estimated that the ensuing transaction lasted about twenty minutes.

14. Black eventually purchased a SNAP card from DHS Special Agent Harris. The card, which was ostensibly assigned to "Maria Sanchez," contained $294.81 in benefits. Black used his cell phone (the "Device") to verify the pre-loaded dollar amount on the SNAP card, and then paid the undercover agent $120.00 in cash for the card. Officers saw Black obtain the $120.00 from another female, who the undercover agent determined was Black's wife. Along with the cash, Black handed the undercover agent a business card for "A.E.C. Marketing and Sales."

15. After the undercover transaction, TPD Officer Josh Metcalf stopped and arrested Black. Officer Metcalf handcuffed Black (in the front because Black recently had shoulder surgery), placed him in a patrol car, and read Black his *Miranda* rights. Black declined to speak with officers, denied that he had a SNAP card (he claimed

that "the lady" had it), and said he did not know why he was being arrested. Officers transported Black to the David L. Moss Criminal Justice Center.

16. After the arrest, TPD Officer Coker and TPD Officer Weis searched Black's vehicle. Officers located a SNAP card that was reported stolen on April 5, 2024. Officers found two additional state assistance cards in the trunk of the car. Later, when Black was being booked into David L. Moss, detention staffer Alyssa Reed found another SNAP card in Black's back pocket.

17. Officers did not locate the SNAP card involved in the undercover transaction (belonging to "Maria Sanchez"). However, law enforcement monitored the card and saw that it was used on Walmart.com later the same day.

18. Officers performed a criminal history check for Robin Black and discovered that he has prior felony convictions, including in California for receipt of stolen property.

19. The Device is currently in the lawful possession of the Tulsa Police Department (TPD). It came into TPD's possession in the following way: the cell phone was seized as part of a search incident to arrest.

20. The Device is currently in storage at a secured facility controlled by the Tulsa Police Department. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Tulsa Police Department.

Technical Terms

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store

their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The

Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include

global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a

range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In addition, this cell phone will likely contain call logs and text messages, which, unless deleted, will contain calls and messages. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. Your affiant knows that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. Your affiant knows that in many cases, cellular telephones maintain photographs of illegal activities, including 7 U.S.C. § 2024(b) – Benefits Fraud. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. Your affiant also knows that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, your affiant knows that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

25. Your affiant knows that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Whatsapp" and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other

important information to the individual. This data includes contacts used to conduct illegal activities to include 7 U.S.C. § 2024(b) – Benefits Fraud.

26. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

27. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

30. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

31. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

32. Affiant requests to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

ERIKA SKAGGS Digitally signed by ERIKA SKAGGS Date: 2024.12.10 10:55:06 -06'00'

Special Agent Erika Skaggs
USDA-OIG

Subscribed and sworn to by phone on December 11th, 2024.

JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a Google Pixel 6a taken off the person of Robin Black incident to his arrest (the "Device"). The Device is currently located in a property room at a secured facility controlled by the Tulsa Police Department, 1111 W. 17th St., Tulsa, Oklahoma, 74107. The Device was turned into the property room under receipt # BW6135.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device described in Attachment A that relate to violations of 7 U.S.C. § 2024(b) – Benefits Fraud, involving Bryce Robin Black, including:

1. Records relating to communication with others as to the criminal offense(s) listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offense(s) listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
3. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offense(s) listed above;
5. All bank records, checks, credit card bills, account information, and other financial records;
6. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
7. Records and information related to the geolocation of the Device and travel in furtherance of the criminal offenses listed above for the time period between October 1, 2023 and May 6, 2024; and
8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this

electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the USDA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.